# Toward New Generation Quantum Cryptography
# -- Japanese strategy --

Masahide Sasaki
National Institute of Information and Communications Technology
Nukuikita, Koganei, Tokyo 184-8795, Japan
Contact email: psasaki@nict.go.jp

## Abstract

We introduce current status of quantum cryptography in Japan, including an inter-city QKD test bed based on DPS-QKD, a field test of one-way BB84 system over 97km with noise-free WDM clock synchronization, and so on. We also discuss how to combine QKD network with photonic network as the essential infrastructure sustaining our society, and extend them into a global network including Space.

## Introduction

Quantum key distribution (QKD) with GHz-range clock rates has recently been demonstrated in various optical transmission systems at around 100km distance or even longer. QKD is now getting into a competitive industry with commercial products. Funding situation in this field may, however, be getting into a kind of recession after strategic funding over 10 years. Now is a time to rethink appropriate promotion schemes and research strategies to cross over the Valley of Death. In this talk I introduce current status of quantum cryptography in Japan, and also discuss what would be the best strategy for promoting quantum cryptography in the next phase.

## Projects in Japan

Fundamental research on quantum information science is mainly promoted by Japan Science and Technology Agency (JST) under the Ministry of Education and Science. R&D of Q-ICT (Information and Communications Technology) for network applications is mainly promoted by NICT under the Ministry of Internal Affairs and Communications. In the following the latter is mainly focused, which is categorized into phases for every 5 years.

Phase I (2001-2005) is to develop key device elements for Q-ICT and to implement prototype of QKD systems. Mitsubishi Electric Corp. demonstrated 96km field QKD in 2005, connecting Kyoto, Nara, and Osaka. The key rate was 8 bps with 10% QBER (Fig.1) [1].

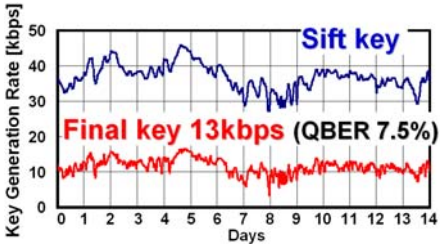


*Figure 1: Final key rate vs elapse times in long term field trial of QKD over a 16 km aerial fiber.*

NEC succeeded in the long term field trial of QKD system for access network. Hands-free run for 14 days over a 16 km aerial fiber was demonstrated, and secret keys were continuously generated at 13kbps for two weeks [2]. These two QKD systems (both was BB84 P&P systems) were combined to a network, and common secret key was successfully shared between two parties, Alice and David (Fig.2).

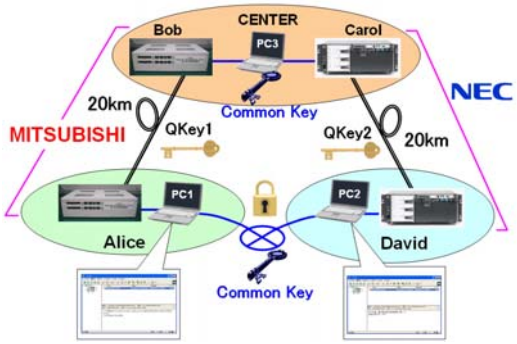


*Figure 2: Interconnection of two different BB84 Plug & Play systems.*

Phase II (2006-2010): The strategic issues by the year 2010 are

(1) To develop a QKD system for metropolitan IP networks within the 50-km range at a secret key rate of 1 Mbps. Networking and WDM technology will also be applied (Commission to NEC and Mitsubishi).

(2) To construct an inter-city QKD test bed exceeding 100 km range at a secret key generate of 10 kbps or higher (Commissioned to NTT).

(3) To develop basic hardware for quantum repeater. Nuclear spins and electron spins in solid will be exploited for the scalability, and entanglement swapping will be demonstrated (Commissioned to NII and NTT).

## Recent results of QKD

Takesue et al. of NTT, NII Stanford division, and NIST have succeeded in transmitting secret keys over 200

km with DPS-QKD system [3]. At 100km, secret keys were as high as 17kbps. A fast clock rate as high as 10 GHz enabled fast key generation. Combination of short pulses of 15 ps with SSPDs with low timing jitter improved SNR significantly, and enabled long distance QKD (Fig.3).

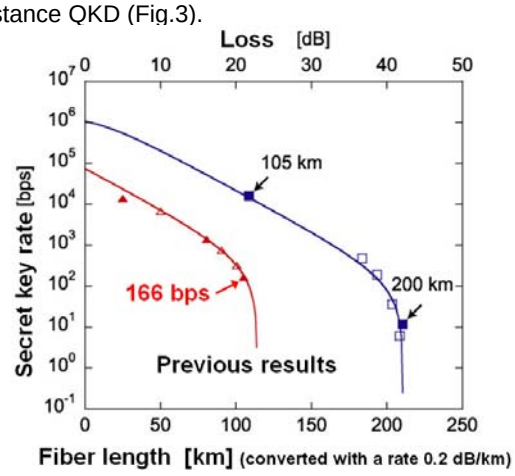


*Figure 3: Secret key rate as a function of (converted) transmission distance.*

NEC, NICT, and NIST have recently put a one-way BB84 system to field test, by applying planar light circuit (PLC), SSPDs, and noise-free WDM clock synchronization [4]. The PLC produces four time-bin signals at 625 MHz repetition. The quantum signal at 1550nm wavelength is combined with the clock signal of 31.25MHz at 1570nm wavelength. They are then transmitted through the same single-mode fiber, installed between Kyoto and Nara in the field network (JGN II). The averaged QBERs were less than 3%, and the averaged sifted key rates were 2.4kbps during 80 minute transmission for 97 km. By applying a decoy state method analysis, the upper bound of secure final key rate is estimated to be about 800 bps (Fig.4).

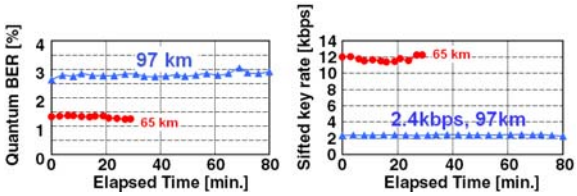


*Figure 4: QBER and sifted key rate as a function of elapsed time.*

To realize real-time secure key generation at a rate higher than 1Mbps over a 50 km range, we need to develop PLC and key distillation board for GHz or higher operation, APD with count rate > 10Mcps, AFP<$10^{-5}$, 6-channel cryocooler SSPD system with count rate > 500Mcps and DE>20%. In the end of Phase II, various QKD systems and related devices will be combined into a fiber-space seamless network in field.

## Toward the next phase

Plans of Phase III (2011~) and IV (2011~) are now under preparation. After Phase III, we should be able to supply products and services which can be advertised as "Quantum inside." To extend QKD network into a practical range, we need to establish scalable quantum repeater technology as well as to pursue space QKD beyond the earth-bound limit.

But a more important thing right now is to consider how to combine QKD network with photonic network as the essential infrastructure, whose backbone traffic will soon reach Peta bps level, and end-to-end access is shifting to 100Gb Ethernet. One possible way of application is to provide secure seed key from QKD layer, to apply fast quantum data encryption with it, and to realize the security at the photonic layer. In Japan, people in both communities have started to discuss R&D promotion strategy in this direction.

Photonic Phase III mainly aims at realizing Photonic Transport Platform based on optical RAM, all optical packet router, one-hop transparent link, and power min photonic NW.

In Quantum Phase III, we should continue research on Q-sources, repeaters, and detectors. We will also demonstrate QKD Service and Q-Data encryption, on Photonic Transport Platform. In the end of Quantum Phase III, Space QUEST will hopefully be launched, and NICT will play a role of the ground station for the inter-continental QKD. Figure 5 is a photo of the world first LEO-to-ground experiment in 2006.

*Figure 5: CCD photo of the world first LEO-to-ground experiment done by NICT in 2006. The bright spot is the beam from the satellite OICETS, while the bright line is uplink from the NICT ground station.*

## References


1. Hasegawa, et al, SCIS2005, EQEC2005.
2. Tanaka, et al., LEOS2005, WM2-3.
3. Takesue et al, Nature Photonics 1, 343 (2007).
4. Tanaka, et al., Opt. Express, 16, 11354 (2008).
5. Miki *et al* App. Phys. Lett. **92** 061116 (2008).